

1 **CLAIMS**

2 What is claimed is:

3 1. A method comprising:

4 determining at least one Squared Tate pairing for at least one hyperelliptic  
5 curve; and

6 cryptographically processing selected information based on said determined  
7 Squared Tate pairing.

8  
9 2. The method as recited in Claim 1, wherein said Squared Tate pairing  
10 is defined for at least one hyperelliptic curve  $C$  of genus  $g$  over a field  $K$ .

11  
12 3. The method as recited in Claim 1, wherein determining said Squared  
13 Tate pairing further includes:

14 forming a mathematical chain for  $m$ , wherein  $m$  is a positive integer and an  
15  $m$ -torsion element  $D$  is fixed on Jacobian of said hyperelliptic curve  $C$ .

16  
17 4. The method as recited in Claim 3, wherein said mathematical chain  
18 includes a mathematical chain selected from a group of mathematical chains  
19 comprising an addition chain and an addition-subtraction chain.

1           5.     A computer-readable medium having computer-implementable  
2 instructions for causing at least one processing unit to perform acts comprising:  
3           calculating at least one Squared Tate pairing for at least one hyperelliptic  
4 curve; and  
5           cryptographically processing selected information based on said determined  
6 Squared Tate pairing.

7  
8           6.     The computer-readable medium as recited in Claim 5, wherein said  
9 Squared Tate pairing is defined for at least one hyperelliptic curve  $C$  of genus  $g$   
10 over a field  $K$ .

11  
12           7.     The computer-readable medium as recited in Claim 5, wherein  
13 determining said Squared Tate pairing further includes:  
14           forming a mathematical chain for  $m$ , wherein  $m$  is a positive integer and an  
15  $m$ -torsion element  $D$  is fixed on Jacobian of said hyperelliptic curve  $C$ .

16  
17           8.     The computer-readable medium as recited in Claim 7, wherein said  
18 mathematical chain includes a mathematical chain selected from a group of  
19 mathematical chains comprising an addition chain and an addition-subtraction  
20 chain.

1           9.     An apparatus comprising:  
2           memory configured to store information suitable for use with using a  
3           cryptographic process;

4           logic operatively coupled to said memory and configured to calculate at  
5           least one Squared Tate pairing for at least one hyperelliptic curve, and at least  
6           partially support cryptographic processing of selected stored information based on  
7           said determined Squared Tate pairing.

8  
9           10.    The apparatus as recited in Claim 9, wherein said Squared Tate  
10          pairing is defined for at least one hyperelliptic curve  $C$  of genus  $g$  over a field  $K$ .

11  
12          11.    The apparatus as recited in Claim 9, wherein said logic is further  
13          configured to form a mathematical chain for  $m$ , wherein  $m$  is a positive integer and  
14          an  $m$ -torsion element  $D$  is fixed on Jacobian of said hyperelliptic curve  $C$ .

15  
16          12.    The apparatus as recited in Claim 11, wherein said mathematical  
17          chain includes a mathematical chain selected from a group of mathematical chains  
18          comprising an addition chain and an addition-subtraction chain.

1           13.    A method comprising:  
2           determining a hyperelliptic curve  $C$  of genus  $g$  over a field  $K$  and a positive  
3 integer  $m$ ;  
4           determining a Jacobian  $J(C)$  of said hyperelliptic curve  $C$ , and wherein each  
5 element  $D$  of  $J(C)$  contains a representative of the form  $A - g(\mathbf{P}_0)$ , where  $A$  is an  
6 effective divisor of degree  $g$ ; and  
7           determining a plurality of functions  $h_{j,D}$  that are iterative building blocks for  
8 the formation of a function  $h_{m,D}$  in order to evaluate  $v_m$  which is a Squared Tate  
9 pairing.

10  
11           14.    The method as recited in Claim 13, wherein said hyperelliptic curve  
12  $C$  is over a field not of characteristic 2.

13  
14           15.    The method as recited in Claim 13, wherein  
15 for at least one element  $D$  of  $J(C)$ , a representative for  $iD$  will be  $A_i - g(\mathbf{P}_0)$ ,  
16 where  $A_i$  is effective of degree  $g$ .

17  
18           16.    The method as recited in Claim 13, wherein if  $P=(x, y)$  is a point on  
19 said hyperelliptic curve  $C$ , then  $-\mathbf{P}$  denotes a point  $-\mathbf{P}=(x, -y)$ , and wherein if a  
20 point  $P=(x, y)$  occurs in  $A$  and  $y \neq 0$ , then  $-\mathbf{P} := (x, -y)$  does not occur in  $A$  and a  
21 representative for identity will be  $g(\mathbf{P}_0)$ .

22  
23           17.    The method as recited in Claim 16, further comprising:  
24 to a representative  $A_i$ , associating two polynomials  $(a_i, b_i)$  which represent a  
25 divisor.

1  
2 18. The method as recited in Claim 16, further comprising:

3 determining  $D$  as an  $m$ -torsion element of  $J(C)$ .

4  
5 19. The method as recited in Claim 18, further comprising:

6 if  $j$  is an integer, then  $h_{j,D} = h_{j,D}(X)$  denoting a rational function on  $C$  with  
7 divisor  $(h_{j,D}) = jA_1 - A_j - ((j-1)g)(P_0)$ .

8  
9 20. The method as recited in Claim 18, wherein  $D$  is an  $m$ -torsion  
10 divisor and  $A_m = g(P_0)$ , and a divisor of  $h_{m,D}$  is  $(h_{m,D}) = mA_1 - mg(P_0)$ .

11  
12 21. The method as recited in Claim 18, wherein  $h_{m,D}$  is well-defined up  
13 to a multiplicative constant.

14  
15 22. The method as recited in Claim 18, further comprising:  
16 evaluating  $h_{m,D}$  at a degree zero divisor  $E$  on said hyperelliptic curve  $C$ ,  
17 wherein  $E$  does not contain  $P_0$  and  $E$  is prime to  $A_i$ .

18  
19 23. The method as recited in Claim 18, wherein  $E$  is prime to  $A_i$  for all  $i$   
20 in an addition-subtraction chain for  $m$ .

21  
22 24. The method as recited in Claim 22, wherein given  $A_i$ ,  $A_j$ , and  $A_{i+j}$ ,  
23 further comprising determining a function  $u_{ij}$  such that a divisor of  $u_{ij}$  is  $(u_{ij}) = A_i$   
24  $+ A_j - A_{i+j} - g(P_0)$ .

1        25.    The method as recited in Claim 22, further comprising:

2        evaluating  $h_{j,D}(E)$  such that when  $j=1$ ,  $h_{1,D}$  is 1.

3  
4        26.    The method as recited in Claim 22, further comprising:

5        given  $A_i$ ,  $A_j$ ,  $h_{i,D}(E)$  and  $h_{j,D}(E)$ , evaluating  $u_{ij}$  to be  $(u_{ij})=A_i + A_j - A_{i+j} -$   
6         $g(\mathbf{P}_0)$ , and  $h_{i+j,D}(E)=h_{i,D}(E) h_{j,D}(E) u_{ij}(E)$ .

7  
8        27.    The method as recited in Claim 13, further comprising:

9        determining a function  $(u_{ij}) = A_i + A_j - A_{i+j} - g(\mathbf{P}_0)$ .

10  
11  
12        28.    The method as recited in Claim 27, wherein  $g = 2$  and

13         $(u_{ij}) = A_i + A_j - A_{i+j} - 2(\mathbf{P}_0)$  is determined as follows

14  
15         $u_{i,j}(\mathbf{X}) := \frac{a_{\text{new}}(x(\mathbf{X}))}{b_{\text{new}}(x(\mathbf{X})) + y(\mathbf{X})} * d(x(\mathbf{X}))$ , if the degree of  $a_{\text{new}}$  is

16  
17        greater than 2, otherwise,  $u_{ij}$  is determined as  $u_{ij}(\mathbf{X}) := d(x(\mathbf{X}))$ , wherein  
18         $d(x)$  is the greatest common divisor of three polynomials  $(a_i(x), a_j(x), b_i(x)+b_j(x))$ .

19  
20  
21        29.    The method as recited in Claim 13, further comprising:

22        determining a Squared Tate pairing for a hyperelliptic curves  $v_m$ , for an  $m$ -  
23        torsion element  $D$  of a Jacobian  $J(C)$  and an element  $E$  of  $J(C)$ , with  
24        representatives  $(\mathbf{P}_1)+(\mathbf{P}_2)+\dots+(\mathbf{P}_g) - g(\mathbf{P}_0)$  and  $(\mathbf{Q}_1)+(\mathbf{Q}_2)+\dots+(\mathbf{Q}_g) - g(\mathbf{P}_0)$ ,  
25

respectively, with each  $\mathbf{P}_i$  and each  $\mathbf{Q}_j$  on the curve  $C$ , with  $\mathbf{P}_i$  not equal to  $\pm\mathbf{Q}_j$  for all  $i, j$ , determining that

$$v_m(D, E) := (h_{m,D}((\mathbf{Q}_1) - (-\mathbf{Q}_1) + (\mathbf{Q}_2) - (-\mathbf{Q}_2) + \dots + (\mathbf{Q}_g) - (-\mathbf{Q}_g)))^{\frac{q-1}{m}}.$$

30. A computer-readable medium having computer-implementable instructions for causing at least one processing unit to perform acts comprising:

determining a hyperelliptic curve  $C$  of genus  $g$  over a field  $K$  and a positive integer  $m$ ;

determining a Jacobian  $J(C)$  of said hyperelliptic curve  $C$ , and wherein each element  $D$  of  $J(C)$  contains a representative of the form  $A - g(\mathbf{P}_0)$ , where  $A$  is an effective divisor of degree  $g$ ; and

determining a plurality of functions  $h_{j,D}$  that are iterative building blocks for the formation of a function  $h_{m,D}$  in order to evaluate  $v_m$  which is a Squared Tate pairing.

31. The computer-readable medium as recited in Claim 30, wherein said hyperelliptic curve  $C$  is not of characteristic 2.

32. The computer-readable medium as recited in Claim 30, wherein for at least one element  $D$  of  $J(C)$ , a representative for  $iD$  will be  $A_i - g(\mathbf{P}_0)$ , where  $A_i$  is effective of degree  $g$ .

33. The computer-readable medium as recited in Claim 30, wherein if  $P=(x, y)$  is a point on said hyperelliptic curve  $C$ , then  $-\mathbf{P}$  denotes a point  $-\mathbf{P}=(x,$

1  $-y)$ , and wherein if a point  $P=(x, y)$  occurs in  $A$  and  $y \neq 0$ , then  $-P := (x, -y)$  does  
2 not occur in  $A$  and a representative for identity will be  $g(P_0)$ .

3  
4 34. The computer-readable medium as recited in Claim 33, further  
5 comprising:

6 to a representative  $A_i$ , associating two polynomials  $(a_i, b_i)$  which represent a  
7 divisor.

8  
9 35. The computer-readable medium as recited in Claim 33, further  
10 comprising:

11 determining  $D$  as an  $m$ -torsion element of  $J(C)$ .

12  
13 36. The computer-readable medium as recited in Claim 35, further  
14 comprising:

15 if  $j$  is an integer, then  $h_{j,D} = h_{j,D}(X)$  denoting a rational function on  $C$  with  
16 divisor  $(h_{j,D}) = jA_1 - A_j - ((j-1)g)(P_0)$ .

17  
18 37. The computer-readable medium as recited in Claim 35, wherein  $D$  is  
19 an  $m$ -torsion divisor and  $A_m = g(P_0)$ , and a divisor of  $h_{m,D}$  is  $(h_{m,D}) = mA_1 - mg(P_0)$ .

20  
21 38 The computer-readable medium as recited in Claim 35, wherein  $h_{m,D}$   
22 is well-defined up to a multiplicative constant.



1           39.    The computer-readable medium as recited in Claim 35, further  
2 comprising:

3           evaluating  $h_{m,D}$  at a degree zero divisor  $E$  on said hyperelliptic curve  $C$ ,  
4 wherein  $E$  does not contain  $P_0$  and  $E$  is prime to  $A_i$ .

5  
6           40.    The computer-readable medium as recited in Claim 35, wherein  $E$  is  
7 prime to  $A_i$  for all  $i$  in an addition-subtraction chain for  $m$ .

8  
9           41.    The computer-readable medium as recited in Claim 39, wherein  
10 given  $A_i$ ,  $A_j$ , and  $A_{i+j}$ , further comprising determining a function  $u_{ij}$  such that a  
11 divisor of  $u_{ij}$  is  $(u_{ij}) = A_i + A_j - A_{i+j} - g(\mathbf{P}_0)$ .

12  
13           42.    The computer-readable medium as recited in Claim 39, further  
14 comprising:

15           evaluating  $h_{j,D}(E)$  such that when  $j=1$ ,  $h_{1,D}$  is 1.

16  
17           43.    The computer-readable medium as recited in Claim 39, further  
18 comprising:

19           given  $A_i$ ,  $A_j$ ,  $h_{i,D}(E)$  and  $h_{j,D}(E)$ , evaluating  $u_{ij}$  to be  $(u_{ij}) = A_i + A_j - A_{i+j} -$   
20  $g(\mathbf{P}_0)$ , and  $h_{i+j,D}(E) = h_{i,D}(E) h_{j,D}(E) u_{ij}(E)$ .

21  
22           44.    The computer-readable medium as recited in Claim 30, further  
23 comprising:

24           determining a function  $(u_{ij}) = A_i + A_j - A_{i+j} - g(\mathbf{P}_0)$ .  
25

45. The computer-readable medium as recited in Claim 44, wherein  $g = 2$  and

$(u_{ij}) = A_i + A_j - A_{i+j} - 2(\mathbf{P}_0)$  is determined as follows

$$u_{i,j}(\mathbf{X}) := \frac{a_{\text{new}}(x(\mathbf{X}))}{b_{\text{new}}(x(\mathbf{X})) + y(\mathbf{X})} * d(x(\mathbf{X})), \text{ if the degree of } a_{\text{new}} \text{ is}$$

greater than 2, otherwise,  $u_{ij}$  is determined as  $u_{ij}(\mathbf{X}) := d(x(\mathbf{X}))$ , wherein  $d(x)$  is the greatest common divisor of three polynomials  $(a_i(x), a_j(x), b_i(x) + b_j(x))$ .

46. The computer-readable medium as recited in Claim 30, further comprising:

determining a Squared Tate pairing for a hyperelliptic curves  $v_m$ , for an  $m$ -torsion element  $D$  of a Jacobian  $J(C)$  and an element  $E$  of  $J(C)$ , with representatives  $(\mathbf{P}_1) + (\mathbf{P}_2) + \dots + (\mathbf{P}_g) - g(\mathbf{P}_0)$  and  $(\mathbf{Q}_1) + (\mathbf{Q}_2) + \dots + (\mathbf{Q}_g) - g(\mathbf{P}_0)$ , respectively, with each  $\mathbf{P}_i$  and each  $\mathbf{Q}_j$  on the curve  $C$ , with  $\mathbf{P}_i$  not equal to  $\pm \mathbf{Q}_j$  for all  $i, j$ , determining that

$$v_m(D, E) := (h_{m,D}((\mathbf{Q}_1) - (-\mathbf{Q}_1) + (\mathbf{Q}_2) - (-\mathbf{Q}_2) + \dots + (\mathbf{Q}_g) - (-\mathbf{Q}_g)))^{\frac{q-1}{m}}.$$

1           47.    An apparatus comprising:  
2           memory configured to store information suitable for use with using a  
3           cryptographic process; and

4           logic operatively coupled to said memory and configured to determine a  
5           hyperelliptic curve  $C$  of genus  $g$  over a field  $K$  and a positive integer  $m$ , determine  
6           a Jacobian  $J(C)$  of said hyperelliptic curve  $C$ , wherein each element  $D$  of  $J(C)$   
7           contains a representative of the form  $A - g(\mathbf{P}_0)$  and  $A$  is an effective divisor of  
8           degree  $g$ , and determine a plurality of functions  $h_{j,D}$  that are iterative building  
9           blocks for the formation of a function  $h_{m,D}$  in order to evaluate  $v_m$  which is a  
10          Squared Tate pairing.

11  
12          48.    The apparatus as recited in Claim 47, wherein said hyperelliptic  
13          curve  $C$  is not of characteristic 2.

14  
15          49.    The apparatus as recited in Claim 47, wherein  
16          for at least one element  $D$  of  $J(C)$ , a representative for  $iD$  will be  $A_i - g(\mathbf{P}_0)$ ,  
17          where  $A_i$  is effective of degree  $g$ .

18  
19          50.    The apparatus as recited in Claim 47, wherein if  $P=(x, y)$  is a point  
20          on said hyperelliptic curve  $C$ , then  $-\mathbf{P}$  denotes a point  $-\mathbf{P}=(x, -y)$ , and wherein if  
21          a point  $P=(x, y)$  occurs in  $A$  and  $y \neq 0$ , then  $-\mathbf{P} := (x, -y)$  does not occur in  $A$  and a  
22          representative for identity will be  $g(\mathbf{P}_0)$ .

1           51.    The apparatus as recited in Claim 50, wherein said logic is further  
2 configured to, for a representative  $A_i$ , associate two polynomials  $(a_i, b_i)$  which  
3 represent a divisor.

4  
5           52.    The apparatus as recited in Claim 50, wherein said logic is further  
6 configured to determine  $D$  as an  $m$ -torsion element of  $J(C)$ .

7  
8           53.    The apparatus as recited in Claim 52, wherein said logic is further  
9 configured to, if  $j$  is an integer, then determine  $h_{j,D} = h_{j,D}(X)$  by denoting a rational  
10 function on  $C$  with divisor  $(h_{j,D}) = jA_1 - A_j - ((j-1)g)(\mathbf{P}_0)$ .

11  
12           54.    The computer-readable medium as recited in Claim 52, wherein  $D$  is  
13 an  $m$ -torsion divisor and  $A_m = g(\mathbf{P}_0)$ , and a divisor of  $h_{m,D}$  is  $(h_{m,D}) = mA_1 - mg(\mathbf{P}_0)$ .

14  
15           55    The apparatus as recited in Claim 52, wherein  $h_{m,D}$  is well-defined  
16 up to a multiplicative constant.

17  
18           56.    The apparatus as recited in Claim 52, wherein said logic is further  
19 configured to evaluate  $h_{m,D}$  at a degree zero divisor  $E$  on said hyperelliptic curve  
20  $C$ , wherein  $E$  does not contain  $\mathbf{P}_0$  and  $E$  is prime to  $A_i$ .

21  
22           57.    The apparatus as recited in Claim 52, wherein  $E$  is prime to  $A_i$  for all  
23  $i$  in an addition-subtraction chain for  $m$ .

58. The apparatus as recited in Claim 56, wherein given  $A_i$ ,  $A_j$ , and  $A_{i+j}$ , and wherein said logic is further configured to determine a function  $u_{i,j}$  such that a divisor of  $u_{i,j}$  is  $(u_{i,j}) = A_i + A_j - A_{i+j} - g(\mathbf{P}_0)$ .

59. The apparatus as recited in Claim 56, wherein said logic is further configured to evaluate  $h_{j,D}(E)$  such that when  $j=1$ ,  $h_{1,D}$  is 1.

60. The apparatus as recited in Claim 56, wherein said logic is further configured to, given  $A_i$ ,  $A_j$ ,  $h_{i,D}(E)$  and  $h_{j,D}(E)$ , evaluate  $u_{i,j}$  to be  $(u_{i,j}) = A_i + A_j - A_{i+j} - g(\mathbf{P}_0)$ , and  $h_{i+j,D}(E) = h_{i,D}(E) h_{j,D}(E) u_{i,j}(E)$ .

61. The apparatus as recited in Claim 47, wherein said logic is further configured to determine a function  $(u_{i,j}) = A_i + A_j - A_{i+j} - g(\mathbf{P}_0)$ .

62. The apparatus as recited in Claim 61, wherein  $g = 2$  and

$(u_{i,j}) = A_i + A_j - A_{i+j} - 2(\mathbf{P}_0)$  is determined by said logic as follows

$$u_{i,j}(\mathbf{X}) := \frac{a_{\text{new}}(x(\mathbf{X}))}{b_{\text{new}}(x(\mathbf{X})) + y(\mathbf{X})} * d(x(\mathbf{X})), \text{ if the degree of } a_{\text{new}} \text{ is}$$

greater than 2, otherwise,  $u_{i,j}$  is determined as  $u_{i,j}(\mathbf{X}) := d(x(\mathbf{X}))$ , wherein  $d(x)$  is the greatest common divisor of three polynomials  $(a_i(x), a_j(x), b_i(x) + b_j(x))$ .

63. The apparatus as recited in Claim 47, wherein said logic is further configured to determine a Squared Tate pairing for a hyperelliptic curves  $v_m$ , for an  $m$ -torsion element  $D$  of a Jacobian  $J(C)$  and an element  $E$  of  $J(C)$ , with representatives  $(\mathbf{P}_1)+(\mathbf{P}_2)+\dots+(\mathbf{P}_g) - g(\mathbf{P}_0)$  and  $(\mathbf{Q}_1)+(\mathbf{Q}_2)+\dots+(\mathbf{Q}_g) - g(\mathbf{P}_0)$ , respectively, with each  $\mathbf{P}_i$  and each  $\mathbf{Q}_j$  on the curve  $C$ , with  $\mathbf{P}_i$  not equal to  $\pm\mathbf{Q}_j$  for all  $i, j$ , and to determine that

$$v_m(D, E) := (h_{m,D} \left( (\mathbf{Q}_1) - (-\mathbf{Q}_1) + (\mathbf{Q}_2) - (-\mathbf{Q}_2) + \dots + (\mathbf{Q}_g) - (-\mathbf{Q}_g) \right))^{\frac{q-1}{m}}.$$